FIPS 140-2 Security Policy for Cisco Aironet LWAPP AP1131AG, Cisco Aironet LWAPP AP1231G, Cisco Aironet LWAPP AP1232AG, and Cisco Aironet LWAPP AP1242AG Wireless Access Points

This security policy contains these sections:

This document may be freely distributed.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Overview

The Cisco Aironet Lightweight AP1131AG, AP1231G, AP1232AG, and AP1242AG (herein collectively called *the modules*) are wireless access points that support the IEEE 802.11a/b/g wi-fi standards for wireless LAN communications, and the IEEE 802.11i standard for wireless LAN security. They are a multiple-chip standalone cryptographic modules, compliant with all requirements of FIPS 140-2 Level 2.

In the FIPS mode of operations, the modules support the Lightweight Access Point Protocol (LWAPP). LWAPP, together with X.509 certificates, authenticates the module as a trusted node on the wired network. All wired network communications for control and bridging traffic are protected with AES encryption. The modules secure all wireless communications with Wi-Fi Protected Access 2 (WPA2). WPA2 is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. The modules use the following cryptographic algorithm implementations:

- AES
- AES-CCM
- SHA-1
- HMAC SHA-1
- X9.31 Random Number Generator
- RSA

This document details the security policy for the lightweight AP1131AG, AP1231G, AP1232AG, and AP1242AG cryptographic modules.

The evaluated platforms are summarized in Table 1.

Table 1 Evaluated Platforms

Model	Firmware Version	Hardware Revision
AP1131AG	3.2.116.21	C0
AP1231G	3.2.116.21	A0
AP1232AG	3.2.116.21	A0
AP1242AG	3.2.116.21	A0

Secure Configuration

This section details the steps used to securely configure the modules to operate in FIPS 140-2 mode of operations. The administrator configures the modules from the wireless LAN controller with which the access point is associated. The wireless LAN controller shall be placed in FIPS 140-2 mode of operations prior to secure configuration of the access points. The Crypto Officer must ensure that the PC that is used for configuring the wireless LAN controller is a stand-alone or non-networked PC.

Follow these steps to prepare the secure configuration for the wireless LAN controller:

Enable FIPS Mode of Operations

The following controller CLI command places the controller in FIPS mode of operations, enabling all necessary self tests and algorithm restrictions:

```
> config switchconfig fips-prerequisite enable
```

Disable Boot Break

The following controller CLI command prevents breaking out of the boot process. It must be executed after enabling FIPS mode of operations.

```
> config switchconfig boot-break disable
```

Configure RADIUS KeyWrap KEK and MACK Keys

The following controller CLI commands configure the RADIUS secret and AES-key wrap KEK and MACK:

```
> config radius auth add index ip-address port hex secret
> config radius auth keywrap add hex kek mack index
> config radius auth keywrap enable
```

Configure Ciphersuites for 802.11i

The following controller CLI commands create a wireless LAN, configure it to use WPA2, associate it with a RADIUS server, and enable it:

```
> config wlan create index ssid
> config wlan security 802.1x disable index
> config wlan security wpa2 enable index
> config wlan radius_server auth add index radius-server-index
> config wlan enable index
```

Set Primary Controller

Enter the following controller CLI command from a wireless LAN controller with which the access point is associated to configure the access point to communicate with trusted wireless LAN controllers operating in FIPS mode.

```
> config ap primary-base controller-name access-point
```

Enter this command once for each trusted controller. Enter **show ap summary** to find the access point name. Enter **show sysinfo** to find the name of a controller.

Save and Reboot

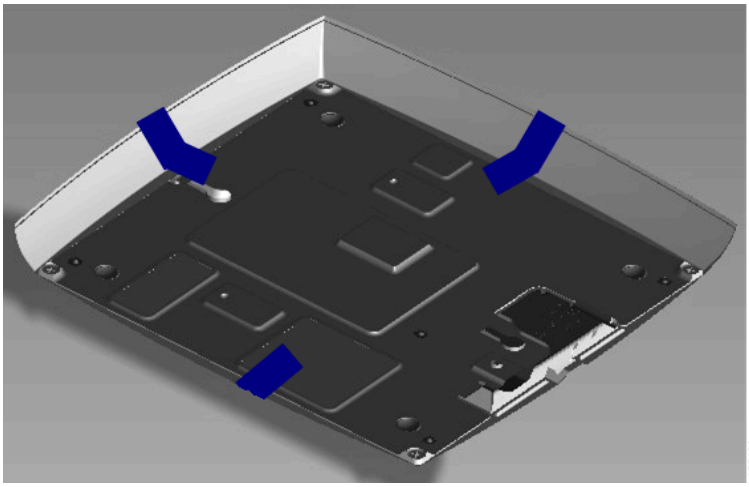
After executing the above commands, you must save the configuration and reboot the system:

```
> save config
> reset system
```

Physical Security Policy

For the AP1131AG, place tamper evident labels over the bottom panel and over the top cover as shown in Figure 1.

Figure 1 Placement of Tamper-evident Labels for the AP1131AG



For the AP1231G, put tamper evident labels over the bottom panel on each of the screws, over the reset button, over the console port and over the panel on the bottom of the module as shown in Figure 2, and place tamper evident labels over the plate on the back of the module as shown in Figure 3. Note that a cap is placed over the reset button in order to prevent it from being pressed. The tamper evident label can be punched so the cap protrudes through it (as pictured) or the cap can be placed entirely underneath the label.

Figure 2 Placement of Tamper-evident Labels on the AP1231G (front view)

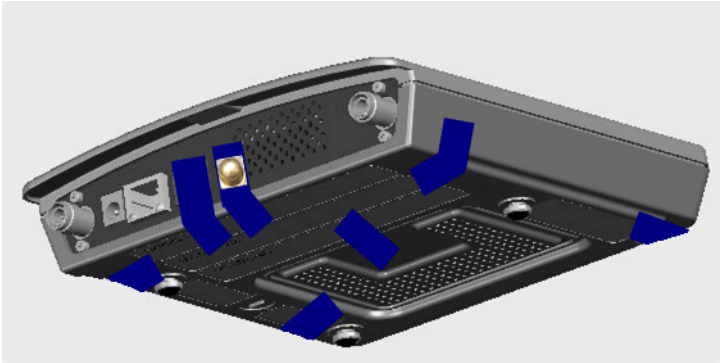
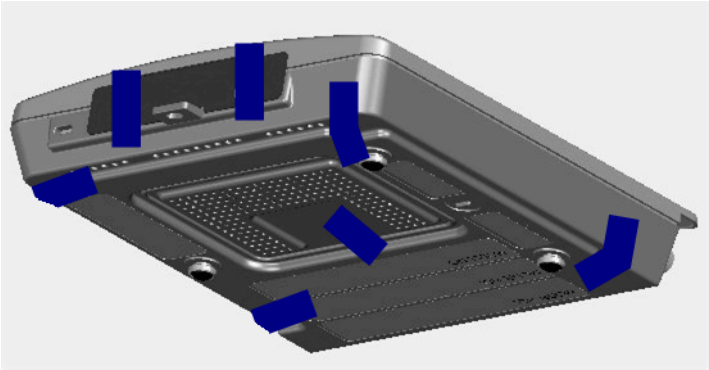


Figure 3 Placement of Tamper-evident Labels on the AP1231G (rear view)



For the AP1232AG, put tamper evident labels over the console port and the reset button as shown in Figure 4, and over the bottom panel on each of the screws, and over the panel on the bottom of the module. Also, place a tamper evident label from the back of the module to the side of the radio card, as shown in Figure 5. Note that a cap is placed over the reset button in order to prevent it from being pressed. The tamper evident label can be punched so the cap protrudes through it (as pictured) or the cap can be placed entirely underneath the label.

Figure 4 Placement of Tamper-evident Labels on the AP1232AG (front view)

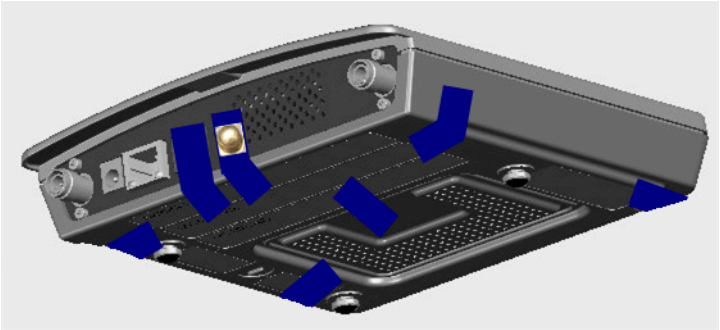


Figure 5 Placement of Tamper-evident Labels on the AP1232AG (rear view)

For the AP1242AG, put tamper evident labels over the removable top cover, over the mode button, and over the console port as shown in Figure 6and Figure 7.

Figure 6 Placement of Tamper-evident Labels for the AP1242AG (Underside of Cover)

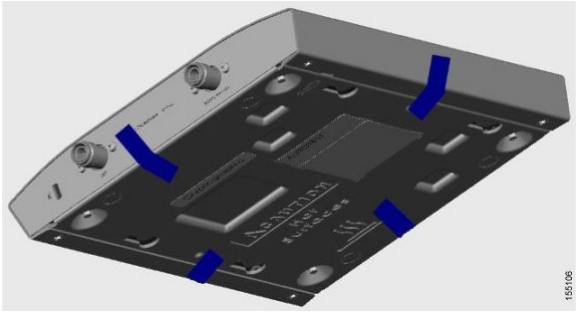


Figure 7 Placement of Tamper-evident Labels for the AP1242AG (Front View)

Roles, Services, and Authentication

This section describes the roles, services, and authentication used by the modules..

Roles

The module supports the roles of Crypto Officer and User. The CO role is fulfilled by the wireless LAN controllers on the network that the module communicates with, and performs routine management and configuration services, including loading session keys and zeroization of the module. The User role is fulfilled by wireless clients. The module does not support a maintenance role.

Services

The services provided are summarized in Table 2.

Table 2 Module Services

Service	Role	Purpose
Self Test and Initialization	CO	Cryptographic algorithm tests, software integrity tests, module initialization. **Note** Module initialization can be obtained either by the CO resetting the access point remotely or by someone with physical access to the module manually cycling the power.
System Status	Any	The LEDs show the network activity and overall operational status.
Key Management	CO	Key and parameter entry, key output, key zeroization.
Module Configuration	CO	Selection of non-cryptographic configuration settings.
LWAPP	CO	Establishment and subsequent data transfer of an LWAPP session for use between the module and the CO.
802.11i	User, CO	Establishment and subsequent data transfer of an 802.11i session for use between the client and the access point.

The modules do not support a bypass capability in the approved mode of operations.

The meaning of the LED indicators on the AP1131AG are summarized in Table 3.

Table 3 LED Status Indicators on the AP1131AG

Sequence	Color Pattern	Status
Power Up	Off	DRAM test in progress
	Green	DRAM test OK
	Off	Board init in progress
	Light Blue	Init flash file system
	Pink	Flash test OK
	White	Init Ethernet
	Blue	Ethernet OK
	Green	Boot software
	Off	Init OK
Power Up Error Indicators	Yellow	Ethernet link down, Ethernet failure, Configuration recovery
	Pink	Image recovery
	Blink Pink/Off	Image recovery in progress
Ongoing Status	Pale Green	Normal with no clients associated
	Blue	Normal with client(s) associated
	Deep Blue	Software upgrade in progress
	Orange	Software failure or error condition
	Blink Green/Off	User set location

The AP1231G and AP1232AG modules have three top panel LEDs that indicate the Ethernet activity, radio activity, and system operational status, and a pair of LEDs on the Ethernet interface that indicates Ethernet activity and line protocol status. Any LEDs blinking yellow or red indicate a warning or error condition.

The AP1242AG module has three LEDs that indicate the Ethernet status, radio status and system operational status. Any LEDs blinking yellow or red indicate a warning or error condition.

Crypto Officer Authentication

The modules authenticate to a wireless LAN controller through the LWAPP protocol, using an RSA key pair with 1536 bit modulus. NIST SP 800-57 defines this modulus size as having effective symmetric key strength of 96 bits, therefore an attacker would have a 1 in 2^{96} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 7.9×10^{23} attempts per minute, which far exceeds the operational capabilities of the modules to support.

User Authentication

Users are authenticated by means of their EAP-TLS key pair and certificates. The RSA key pair for the EAP-TLS credentials has modulus size of 1024 bit to 2048 bit, thus providing between 80 bits and 112 bits of strength. Assuming the low end of that range, an attacker would have a 1 in 2^{80} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately $1.8x10^{21}$ attempts per minute, which far exceeds the operational capabilities of the modules to support.

Cryptographic Key Management

Cryptographic keys are stored in flash and in SDRAM for active keys.

No keys are generated in the module. All keys are input into the module from the controller over an LWAPP session. During an LWAPP session, the APs first authenticate to the Wireless LAN controller using an RSA key pair. After a successful authentication, the LWAPP session key generated in the controller is transported from the controller to the module wrapped with AP's RSA key. The GTK and TK are input into the module encrypted with the LWAPP session key over an LWAPP session. The GTK and TK are the 802.11i session keys and are used by the module to encrypt 802.11i traffic. The module does not output any plain text cryptographic keys.

Table 4 lists the secret and private cryptographic keys and CSPs used by the modules. Table 5 lists the public keys used by the modules. Table 6 lists the access to the keys by services.

Table 4 Secret and Private Cryptographic Keys and CSPs

Name	Algorithm	Storage	Description and Zeroization
PRNG seed key	X9.31	SDRAM	This is the seed key for the PRNG. It is zeroized during the zeroization procedure.
PRNG seed	X9.31	SDRAM	This is the seed for the PRNG. It is zeroized during the zeroization procedure.
cscoIdCert key	RSA	Flash	This is the AP's RSA private key. It is zeroized during the zeroization procedure.
LWAPP Session Key	AES-CCM	SDRAM	The session key used to authentication and encrypt LWAPP traffic. It is zeroized during the zeroization procedure.[1]
802.11i Temporal Key (TK)	AES-CCM	SDRAM	The TK, also known as the CCMP key, is the 802.11i session key for unicast communications. It is zeroized during the zeroization procedure.
802.11i Group Temporal Key (GTK)	AES-CCM	SDRAM	The GTK is the 802.11i session key for broadcast communications. It is zeroized during the zeroization procedure.

1. RSA key wrapping provides 96 bits of effective symmetric key strength.

Table 5 Public Keys

Name	Algorithm	Storage	Description and Zeroization
bsnOldDefaultCaCert	RSA	Flash	Verification certificate, used with LWAPP to authenticate the controller. It is zeroized during the zeroization procedure.
bsnDefaultRootCaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations. It is zeroized during the zeroization procedure.
bsnDefaultCaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations. It is zeroized during the zeroization procedure.
cscoDefaultNewRootCaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations. It is zeroized during the zeroization procedure.
cscoDefaultMfgCaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations. It is zeroized during the zeroization procedure.
cscoIdCert	RSA	Flash	This is the AP's RSA public key.

Table 6 Key/CSP Access by Service

Service	Key Access
Self Test and Initialization	• Initializes PRNG Seed
System Status	• None
Key Management	• Zeroize cscoIdCert
Module Configuration	• None
LWAPP	• Authenticate to controller using cscoIdCert Private Key • Authenticate controller using bsnOldDefaultCaCert • Establish LWAPP Session Key and then encrypt/decrypt LWAPP control traffic with Session Key • Encrypted TK and GTK entry from controller for 802.11i service
802.11i	• Encrypt/decrypt using TK, GTK

Key Zeroization

All keys in the modules may be zeroized by entering this command on the controller to which the access point is associated:

```
> config switchconfig key-zeroize ap ap-name
```

Disallowed Security Functions

These cryptographic algorithms are not approved, and may not be used in FIPS mode of operations:

- RC4
- MD5
- HMAC MD5

Self Tests

The following self tests are performed by the module:

- Firmware integrity test
- Power on self test of AES, AES-CCM, SHA-1, HMAC SHA-1, RNG and RSA algorithms
- Continuous random number generator test for Approved and non-Approved RNGs

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html